NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

IN THE MATTER OF

STANDARD CHARTERED BANK and
STANDARD CHARTERED BANK, NEW YORK BRANCH

CONSENT ORDER UNDER NEW YORK BANKING LAW §§ 39 and 44

The New York State Department of Financial Services (the "Department"), Standard Chartered Bank, and Standard Chartered Bank, New York Branch (together, "Standard Chartered" or "the Bank") are willing to resolve the matters described herein without further proceedings.

WHEREAS, Standard Chartered is a global financial institution headquartered in London, England, and is part of the Standard Chartered group, with more than $663 billion in total assets and employing approximately 86,000 individuals worldwide;

WHEREAS, Standard Chartered (or a predecessor entity) has been licensed by the Department to operate a foreign bank branch since 1976 ("SCB-NY" or the "New York Branch"), which as of December 31, 2018 held more than $40 billion in total assets;

WHEREAS, the Department has been investigating Standard Chartered relating to U.S. dollar clearing services for the benefit of Iranian parties and parties from other sanctioned countries;

WHEREAS, the Department and Standard Chartered are willing to resolve the matters described herein without further proceedings. The Department hereby finds as follows:

THE DEPARTMENT'S FINDINGS AFTER INVESTIGATION

1. **The Prior Sanctions Investigation**: On September 21, 2012, pursuant to a consent order with the Department (the "2012 Consent Order"), the Bank admitted to the practice of intentionally "stripping" information – removing or omitting -- from payment messages that concerned Iranian parties or destinations for transactions processed through the New York Branch.

2. The practice was euphemistically known as "repair": a process, approved at the highest levels of the Bank's management, to systematically delete information from "SWIFT" payment messages that would identify Iranian parties and locations.[1] During the period January 2001 through 2007, the Bank provided U.S. dollar ("USD") clearing services to Iranian banks, corporations and individuals, processing non-transparent transactions of approximately $250 billion.

3. The Department determined that this type of non-transparent conduct posed serious sanctions risks. This practice interfered with the Department's ability to perform effective safety and soundness examinations. It also prevented the Department from identifying suspicious activity that could assist the Department in effectively supervising other licensed institutions, and from assisting other law enforcement authorities. This misconduct was the basis for the violations of law set forth in the 2012 Consent Order.

4. In 2011 and again in 2012, during the course of the Department's prior investigation, the Bank assured the Department that, since 2007, the Bank had made significant progress in reforming its sanctions compliance function.

[1] The Society of Worldwide Interbank Financial Telecommunications ("SWIFT") is a communications network through which banks exchange wire transfer messages with other financial institutions, including U.S. correspondent banks. SWIFT messages contain various informational fields useful in identifying parties to the transactions.

5. **The Current Sanctions Investigation**: The Bank's confidence in its improvements was unjustified. Additional investigation undertaken by the Department since 2013 (the "Department's Investigation" or "Investigation") has determined that, from 2008 through 2014, a still notably inadequate sanctions compliance function, both at the Bank's Home Office and at its Dubai branch, allowed for the processing of an additional $600 million in USD payments that violated regulations issued by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"), and thus resulted in violations of New York laws and regulations as well.

6. The vast majority of these payment messages originated from clients in (or ordinarily resident in) Iran, at a time that these transactions were strictly prohibited by U.S. law. These transactions were transmitted to the Bank through its fax payment system at the Dubai branch, or directly through the Bank's online banking platform. A large majority of these $600 million in illegal USD payments transited through the New York Branch – several dozen occurring as late as 2014.

7. The Department's Investigation identified (a) significant gaps in the Bank's payment systems controls, (b) incomplete customer due diligence ("CDD") files, (c) inadequate leadership within the Group Sanctions and Compliance functions, and (d) thin oversight of employees at the Bank's Dubai branch. These deficiencies permitted persistent illegal conduct; in the face of significant exposure in a high-risk jurisdiction, and despite its assurances to the Department, the Bank's attempts to ensure compliance with U.S. sanctions law were far from adequate. For these reasons, this enforcement action is warranted.

Prior DFS Investigations Involving Standard Chartered's Sanctions and Anti-Money Laundering Compliance Programs

The 2012 Consent Order

8. From January 2010 through August 2012, the Department undertook an investigation of Standard Chartered's USD clearing business. The investigation concerned the Bank's systematic and intentional stripping of information contained in the "SWIFT" inter-bank communication messages in order to conceal the fact that Iranian entities were parties to dollar-denominated transactions clearing through the New York Branch – a practice known as "wire stripping."

9. Although some of these payment transactions might have been permissible under U.S. law under an exception known as the "U-turn" exemption, all of the transactions at issue in the Department's initial investigation were improperly shielded by the Bank from review by the Department, and thus non-transparent.[2]

10. The wire stripping carried out by the Bank violated a number of New York laws and regulations, because it completely thwarted required transparency and prevented the Department from conducting appropriate examinations and supervision to ensure the Bank was acting in a safe and sound manner. The conduct was deliberate, masking approximately $250 billion in USD transactions flowing through the New York Branch between 2001 and 2007. Additionally, a substantial sum of the Bank's USD transactions that cleared through the New

[2] As relevant here, in early 1995 President Clinton, acting pursuant to International Emergency Economic Powers Act ("IEEPA"), issued Executive Order 12957, which severely restricted trade and investment activities between the United States and Iran. While subsequent executive orders strengthened these restrictions, for a period of time federal law excepted from these limitations certain transactions. One exception, effective until November 2008, authorized U.S. financial institutions to process certain funds transfers for the direct or indirect benefit of Iranian banks, other persons in Iran, and the Government of Iran, provided that such payments were initiated offshore by a non-Iranian, non-U.S. financial institution and only passed through the U.S. financial system en route to another offshore, non-Iranian, non-U.S. financial institution ("U-Turn" transactions). *See* https://www.treasury.gov/press-center/press-releases/Pages/hp1257.aspx.

York Branch also constituted violations of federal economic sanctions laws, therefore violating New York laws and regulations as well.

11. As a result of the Bank's conduct, the Department and the Bank entered into the 2012 Consent Order to resolve the Department's investigation. Under the 2012 Consent Order, the Bank agreed to (a) pay a civil monetary penalty of $340 million; (b) undertake significant remediation of its sanctions compliance program; and (c) install an independent monitor appointed by the Department, which would make recommendations about remediation and oversee its implementation at the Bank (the "Monitor").

12. As noted above, the period subject to scrutiny during the prior investigation was the years 2001 through 2007 (the "Review Period"). In November 2011, the Bank represented to the Department that, "since the Review Period, [the Bank] has significantly enhanced all areas of its sanctions compliance program, including policies and procedures, customer due diligence, transaction and customer screening, resources, training and assurance. . . . [The Bank] has also made substantial investments in improving the systems critical to Sanctions compliance."

The 2014 Consent Order

13. While examining the Bank's systems in 2013 and 2014, the Department's Monitor identified serious flaws in the Bank's transaction monitoring system which had a direct and negative impact on the efficacy of the New York Branch's compliance function. The Monitor determined that the rules governing the transaction monitoring system failed to detect a significant number of potentially high-risk transactions that should have been subjected to further review by Compliance staff.[3]

[3] Transaction monitoring, an essential component of the compliance function, is the process by which an institution monitors financial transactions after their execution for potential Bank Secrecy Act or Anti-Money Laundering ("BSA/AML") violations, and determines whether there should be any Suspicious Activity Reports ("SARs") filed with law enforcement authorities.

14. Given the serious nature of these further violations of New York laws and regulations, the Department and the Bank entered into a second Consent Order on August 19, 2014 (the "2014 Consent Order") to resolve this additional conduct by the Bank. Among other things, the Bank agreed to (a) pay a civil monetary penalty of $300 million; (b) undertake significant remediation, this time to the Bank's anti-money laundering program; and (c) continuation of the work of the Monitor.

Prohibited Transactions with Iranian Parties During the Period 2008 through 2014

Customers Continued Using the Bank's Internet Banking Platform from Iran

15. As early as 2004, the U.S. Treasury Department warned financial institutions of compliance risks presented by banking services accessed by bank customers via the internet.[4] Even prior to the 2012 Consent Order, senior compliance managers at the Bank were aware that USD payment requests from Iran could be transmitted electronically via the Bank's "iBanking" and "Straight-to-Bank" or "S2B" internet platforms, and that the Bank had no effective mechanism to detect or block such channels.

16. For example, in May 2010, a senior anti-money laundering officer at the Bank's branch in Dubai, United Arab Emirates (the "Senior Dubai AML Officer"), warned a senior financial crime risk officer for the UAE (the "Senior UAE FCR Officer") that the Bank was exposed to substantial risk from Iranian USD payment requests entering its online banking systems. The Senior Dubai AML Officer stated in an e-mail, "***the added risk that we have to live with that if the transactions were originated through iBanking [where] there is no way of***

[4] *See, e.g.*, OFAC FAQ No. 73, *Compliance for Internet, Web Based Activities, and Personal Communications* (Apr. 13, 2004) https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx. ("[A] number of internet-based financial institutions already developed Internet Protocol (IP) address blocking procedures. . . . Users attempting to initiate an online transaction or access an account from a sanctioned country are blocked based on their IP address. While this approach is effective, it does not fully address an internet firm's compliance risks[.].")

us knowing whether the issuer of such transactions was in Iran when he [e]ffected [the payment]."

17. Later, in October 2012, a senior sanctions officer in the U.S. (the "Senior U.S. Sanctions Officer") acknowledged, in an e-mail to a senior sanctions officer in the U.K. (the "Senior U.K. Sanctions Officer"), that ***"not blocking access from sanctioned countries makes it easier for clients to open an account posing as being based in one country when they are really based in another***."

18. Further, on a number of occasions between 2010 and 2012, experienced staff within Group Compliance expressed concrete concerns to senior managers that the Bank was at risk of infiltration by Iranian parties through its online banking platform. Senior managers who were made aware of this significant risk include (a) the Senior UAE FCR Officer, (b) the Senior U.S. Sanctions Officer, and (c) a senior member of the Bank's executive management team (the "Senior Executive") who reported directly to the CEO.

19. Between November 2008 and 2012, the Bank's failure to block online banking access permitted more than 100 customers to conduct USD transactions from Iran and other sanctioned countries through the iBanking and S2B platforms. And between June 2009 and mid-2014, the Bank processed more than $275 million in online banking transactions from Iran, Myanmar, Sudan, Syria and Cuba, in direct violation of OFAC regulations.

20. In approximately March 2012, Group Compliance staff discovered that dozens of Bank clients had used S2B to access USD accounts from Iran. At the time, Bank IT personnel informed the Senior UAE FCR Officer that, "***If the business agrees, IP [internet protocol] addresses from Iran can be blocked***."

21. Because "the business" did not agree, the Bank's response to this discovery was slow and inadequate. Although each was authorized to do so at the moment they were notified of this discovery in March 2012, neither the Senior U.S. Sanctions Officer nor the Senior U.K. Sanctions Officer took steps necessary to ensure the Bank began immediately blocking S2B access from Iran. Nor did either of these senior executives direct an immediate transactional review of payments already processed from Iran via S2B. Doing so would have provided an understanding of which customers had been accessing S2B to make USD payments from Iran, which would have permitted the Bank to terminate these customers and report these illegal activities to the Department, OFAC and other appropriate authorities.

22. Instead, the Senior U.S. Sanctions Officer and Senior U.K. Sanctions Officer proceeded in a "business-as-usual" fashion, undertaking a sluggish effort to persuade business managers to implement blocking of access to the S2B platform from IP addresses located in Iran and other sanctioned countries.

23. It was not until 2014 -- when the Department and other agencies were investigating the Bank's transactions with Iran after 2007 -- that the Bank finally commenced a review of S2B transactions originating from customers in sanctioned countries. And only in July 2014 did the Bank comprehensively disable access to USD banking channels available via the internet from these sanctioned nations – more than two years after discovery of this risk.

Faxed Payment Requests Originating in Iran

24. In late 2009, the Senior Dubai AML Officer discovered that the Bank's "Right Fax" system, a basic system of receiving payment instructions from customers who transmitted them to the Dubai branch by facsimile, could facilitate USD payments initiated by requests originating in Iran. Faxed payment instructions frequently bore an electronic header that

contained the originating fax machine's telephone number, including a "+98" Iranian country code. The Senior Dubai AML Officer then sent an e-mail to nearly all sanctions and compliance managers responsible for the UAE region, including the Senior U.K. Sanctions Officer, advising them that: "[w]e can receive [payment] instructions via [R]ight [F]ax . . . ***a check will have to be done here [to discover] whether these fax numbers begin with the Iran [country] code +98***."

25. Subsequently, the Senior Dubai AML Officer drafted what became known as the "Iran Addendum." The Iran Addendum sought to implement enhanced due diligence for the Bank's customers that were Iranian nationals. Among other things, it would have required Bank staff to conduct a periodic sampling of the headers on incoming Right Fax payment messages in order to screen for the Iranian "+98" country code. However, complaints from the Bank's UAE business staff regarding the purported burden of such a review persuaded the Senior U.K. Sanctions Advisor to remove this screening requirement from the Iran Addendum.

26. In the Spring of 2010, others who reviewed the Iran Addendum (and unlike the UAE business staff) suggested to sanctions and compliance managers that "***there should be a system enhancement on [R]ight [F]ax that should trigger up any faxes received with the +98 country code.***" Also about this time, an operational risk and process manager in the Bank's Dubai branch asked the sanctions and compliance team whether faxes from Iran could be blocked altogether, or flagged for rejection, to avoid processing illegal Iranian payments: "***It is ideal to have alert mechanisms" which would "not allow [or] put a refer marker [on] any transactions faxed from Iran.***"

27. Similarly, at about the same time in 2010, a process development manager for Consumer Banking suggested to the Senior U.K. Sanctions Officer and others that the Bank should require UAE employees receiving faxed payment instructions to "***check the country code***

from where the instructions are received and advise them to 'reject' if it is received from Iran."

28. Despite a vivid recognition that the Right Fax system posed a substantial sanctions risk, the Bank's senior compliance managers again failed to take additional steps to block or better identify faxed USD payment messages originating in Iran. Although certain other measures subsequently taken by the Bank helped reduce this sanctions risk, the Right Fax system remained available for effectuating illegal payments from Iran until as late as May 2014.

29. Not until May 2014 did the Bank initiate a systems change in the UAE to prevent the Right Fax system from receiving transmissions from Iran and other sanctioned countries. Notably, the process for blocking fax transmissions from Iran to the Bank's Dubai branch – something that had been recommended nearly two years before -- took less than a week to implement.

Iranian Front Companies

30. The Department discovered through a separate investigation that Standard Chartered continued to process a significant volume of USD payments for at least one customer at the Dubai branch -- a front company for a prohibited Iranian entity -- for years after OFAC's November 2008 revocation of the U-Turn exemption. The prohibited entity was an Iranian petrochemical company in the business of shipping liquefied petroleum gas ("Front Co. 1").

31. From 2005 through 2012, the Bank provided services to Front Co. 1 via its Dubai branch. While holding itself out as being operated from Dubai, Front Co. 1 was, in fact, a front company whose sole beneficial owner was an Iranian national. Between November 2008 and June 2012, the Bank processed more than $150 million in incoming and outgoing USD

transactions for Front Co. 1, the majority of which were transmitted through the New York Branch.

32. A number of glaring compliance deficiencies at the Bank allowed for this prohibited business to continue. For example:

- The Bank failed to conduct sufficient CDD on Front Co. 1's Dubai account, thus preventing compliance managers from recognizing that Front Co. 1's sole beneficial owner was already known to the Bank as an Iranian national.[5] Additionally, Bank personnel failed to update Front Co. 1's account file with a valid UAE residency visa, instead relying on the account owner's expired UAE visa that had not been updated since 2005.

- Bank personnel at the Dubai branch failed to connect Front Co. 1 to a rejected letter of credit application of its sole owner at the Bank's Tehran representative office. The application had been rejected at the Tehran representative office due to the same owner's stake in a known Iranian gas company.

- The Senior U.K. Sanctions Officer also failed repeatedly to heed red flags raised by his own staff and other financial institutions. For example, in April 2010 another global financial institution, acting as a beneficiary bank, rejected a large USD payment processed by the Bank on behalf Front Co. 1. The other bank conveyed to compliance staff at the New York Branch that its rejection was based on the other bank's research, and warned Standard Chartered's New York Branch that it "kn[ew] [Front Co. 1] to be an Iranian entity," had "contacted OFAC, and was advised by OFAC to reject [USD] payments." These warnings were transmitted to the Senior U.K. Sanctions Officer immediately, who did nothing.

- On the following day an operational risk manager at Standard Chartered's Dubai branch conducted research on Front Co. 1's account and discovered: (i) the sole beneficial owner was an Iranian national; (ii) the owner's UAE visa had expired two years earlier; (iii) an online Google search of Front Co. 1 indicated that Front Co. 1, with the same name and e-mail address as that on record with the Bank, was "Iranian," and (iv) a document in Front Co. 1's account file from 2008 revealed its representative office was located in Tehran, Iran.

- The operational risk manager in Dubai escalated those concerns about Front Co. 1 to the Senior Dubai AML Officer, warning that, based on this research, the manager "strongly believe[d] that the subject customer is an Iranian." The Senior Dubai AML Officer, in turn, escalated the findings to the Senior U.K. Sanctions Officer -- who then

[5] In 2005, the Bank put a marker on the personal bank account of Front Co. 1's sole shareholder, at the Dubai branch, tagging it as "Iranian" owned, and in 2007 blocked the account from transacting in any currency due to Iranian ties. The Bank conducted no due diligence to connect the blocked personal account to Front Co. 1's business account, even though both were owned by the same individual.

rejected this warning, allowing the payment to be made by relying on an undocumented assertion of a UAE relationship manager that Front Co. 1's owner, when reached for an explanation, denied that his business had any "links with Iran."

- The Senior U.K. Sanctions Officer also failed to act on a fax communication located in Front Co. 1's account file that contained correspondence from Iran. The fax, sent to the Bank in September 2011, bore an Iranian country code stamp of +98. Again, the Senior U.K. Sanctions Officer inexplicably gave Front Co. 1 the benefit of the doubt and allowed it to continue conducting business through the Bank – including transactions processed through the New York Branch.

33. This significant compliance failure persisted until March 2012, when other Bank employees in the business line scrutinized Front Co. 1's obvious ties to Iran and finally authorized steps to close the account on that basis. But this series of events was not isolated.

34. For example, in another instance involving an Iranian front company customer, a relationship manager in the Bank's Dubai branch ("RM 1") improperly took money in 2010 from the account's beneficial owner in order to a buy a personal car. The payment to RM 1 passed through his personal bank account at the Bank, as well as the Iranian entity's account at the Bank's Dubai branch, without detection by the Bank for years.

35. In 2011, the Bank closed the original USD account for this Iranian front company customer on the basis of its sanctions risk. Using his Standard Chartered e-mail account, RM 1 wrote to the Iranian front company customer, "***Last year you helped me for getting my car for which I am always thankful to you***." RM 1 then helped re-open a USD account for the Iranian front company customer at the Dubai branch under a different corporate name. To assist the Iranian customer in avoiding detection by the Bank, RM 1 advised the customer to avoid using the original company e-mail address and phone number for the account opening paperwork, as well as any reference to the name of the company that now had the closed account.

36. RM 1 also warned another Iranian front company's owner that it should close its account before the Bank reported it as suspicious: "***before [the Bank] report[s] to [the local***

bank regulator] . . . please can you send me a closure notice before [the Bank] raise question on you?"

37. A different relationship manager ("RM 2") also advised an employee of Front Co. 1 on how to evade detection as a sanctioned entity: "***if you change the company name then we can reopen another account with Standard Chartered***."

Volume of Additional Impermissible Transactions

38. The Department's Investigation determined that, during the period November 2008 through July 2014, the Bank processed nearly 15,000 illegal payments for the benefit of sanctioned Iranian parties, totaling more than $600 million. The Bank also conducted an additional $20 million in USD payments for illegal transactions involving Syrian, Sudanese, Burmese and Cuban entities. A majority of these transactions flowed through the New York Branch, and none were permitted under the "U-turn" exemption.

Standard Chartered's Deficient Sanctions Compliance Program and Overconfidence Allowed the Illegal Iranian Business to Continue

39. Prior to early 2014, the Bank offered repeated assurances to the Department about the purportedly substantial improvements it was making to its sanctions compliance program. In November 2011, for example, the Bank assured the Department that Group Sanctions Compliance could adequately manage its sanctions risk, asserting that "[a]n exhaustive investigation of [the Bank's] conduct from 2001 to 2007 shows that there were diligent efforts to comply with U.S. sanctions regulations. . . . . [The Bank] expended significant time and resources to ensure that its Iranian business complied with OFAC regulations." The Bank further represented that it had significantly enhanced all areas of its sanctions compliance program, including policies and procedures, customer due diligence, transaction and customer

screening, resources, training and assurance, and "[had] also made substantial investments in improving the systems critical to sanctions compliance."

40. Similarly, in Summer 2012, the Bank highlighted a Sanctions Compliance Program that it said would strengthen controls in the critical areas of governance, policies and procedures, training and assurance, from the business level up to the highest levels of Group management. The Bank further represented to the Department that sanctions screening improvements included "automated screening of cross-border SWIFT messages to and from all [Bank] offices," and "increased focus on development of internal [Bank] watch lists."

41. In light of these supposed enhancements, the Bank determined that it would continue servicing customers in jurisdictions that posed substantial risks for ensuring compliance with U.S. sanctions laws, including the UAE. Until the end of 2013, the Bank's policy at its Dubai branch was to permit as customers Iranian nationals seeking to open USD accounts for small-to-medium enterprises ("SMEs"), so long as the owners completed CDD requirements, including providing UAE residency visas, and were not majority shareholders of the businesses they owned.

42. The Department's Investigation further revealed that, as a general matter, the Bank's compliance infrastructure in the UAE region was woefully inadequate. Client-facing and compliance staff were poorly trained and unconcerned with complex U.S. sanctions regulations. Business personnel could not keep up with the due diligence reviews recommended by the Iran Addendum, resulting in a significant backlog in CDD checks by relationship managers in the Dubai branch.

43. Thus, the Bank's sanctions controls at the Dubai branch were no match for even unsophisticated evasion efforts. Many of the CDD files at the Bank's Dubai branch were wholly

inadequate, missing for example, critical information and key documents such as a valid UAE residency visa.

44. In May 2011, a senior compliance officer in the U.S. recommended a limited review of 19 specific SMEs at the Dubai branch, due to an identified sanctions risk based on the type of company involved, *i.e.,* a general trading company. A senior manager of SME Banking for the Middle East confirmed this risk, stating in early 2012 in an e-mail to a very senior SME banker (the "Senior SME Banker"), ***"[M]any of our [Dubai branch] customers are (a) Iranian nationals (owners of SMEs), (b) Selling to Iran . . . (c) Supplying to local buyers who have customers in Iran. . . . 814 SME customers have Iranian owners. They may or may not have any direct/indirect exposure to Iran***."

45. However, the Senior UAE FCR Officer dismissed the request, stating, "All accounts where there is an Iranian national involvement conform with our policy that if they are resident in the UAE then we are able to deal with them . . . ." As a result, the Dubai branch ultimately reviewed only five of the SMEs recommended for review. Of the 14 companies not reviewed by compliance, two proved to be responsible for approximately $100 million in illegal Iranian transactions conducted by the Bank between November 2008 and 2012. In sum, the Bank's still inadequate sanctions compliance program, including at its Dubai branch, was a root cause of its persistence after 2007 in engaging in illegal payments to and from Iran and other sanctioned countries.

Cooperation and Remediation

46. The Department recognizes the Bank's very substantial cooperation with the Department's Investigation, including presentations of the Bank's own internal investigation, appropriate responses to the Department's requests for information, the production of a

voluminous quantity of documents, making witnesses available for interviews, and responses to additional inquiries from the Department.

47. The Department recognizes that, since in or about 2014, the Bank has undertaken significant remediation, including by implementing more robust sanctions policies, procedures, and programs, and through the hiring of new senior leadership and staff in its legal and financial crime compliance functions. These changes have fostered an improved culture of compliance and marked enhancements to the Bank's financial crime compliance function. The Department has given substantial weight to this cooperation and remediation described in Paragraphs 46-47 in agreeing to the terms and remedies of this Consent Order, including the civil monetary penalty imposed.

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Sections 39 and 44 of the Banking Law, the Department and the Bank hereby stipulate and agree to the terms and conditions below requiring further review of the Bank's activities, for remediation, and for imposition of a penalty:

VIOLATIONS OF LAWS AND REGULATIONS

48. The Bank conducted business in an unsafe and unsound manner, in violation of New York Banking Law § 44.

49. The Bank failed to maintain an effective and compliant OFAC compliance program, in violation of 3 N.Y.C.R.R. § 116.2.

50. The Bank failed to maintain and make available appropriate books, accounts, and records, reflecting all transactions and actions, in violation of New York Banking Law § 200-c.

51. The Bank failed to submit a report to the Superintendent immediately upon discovering fraud, dishonesty, making of false entries or omission of true entries, or other misconduct, whether or not a criminal offense, in violation of 3 N.Y.C.R.R. § 300.1.

52. The Bank failed to submit a report to the Superintendent of one or more incidents that appear to relate to a plan or scheme that would be of interest to similar organizations located in the same area or through the state, in violation of 3 N.Y.C.R.R. § 300.4.

SETTLEMENT PROVISIONS

Monetary Penalty

53. The Bank shall pay to the Department a civil monetary penalty pursuant to Banking Law § 44 in the amount of $180,000,000. The Bank shall pay the entire amount within ten (10) days of executing this Consent Order. The Bank agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

Employee Discipline

54. The Bank has undertaken an accountability review of current and former employees for conduct identified in or related to the Department's Investigation (the "Conduct Review"). As a result of the Conduct Review and other efforts by the Bank in the course of the Department's Investigation, the Bank has applied certain discipline or consequences for those employees identified as having engaged in certain misconduct or behavior in the Conduct Review, including termination of seven employees. Additionally, 14 individuals involved in the misconduct identified in the Department's Investigation resigned from the Bank or were otherwise terminated due to unrelated reasons, prior to the time any disciplinary action might have been taken against them by Standard Chartered.

55. The Bank shall not in the future, directly or indirectly, rehire or retain as an officer, employee, agent, consultant, or contractor of the Bank or any affiliate of Standard Chartered, or in any other capacity, the following: (a) the Senior Executive, (b) the Senior U.S. Sanctions Officer, (c) the Senior U.K. Sanctions Officer, or (d) any individual that the Bank has tagged in its human resources records as "Do Not Rehire – Misconduct" as a result of the Conduct Review.

Remediation for Standard Chartered's Sanctions Compliance Program

Continuation of Independent Consultant

56. As set forth in the Second Supplemental Order dated November 21, 2018 between the Bank and the Department (the "2018 Consent Order"), commencing January 1, 2019, and for a period of up to one year (with the Department retaining sole discretion to extend the time period for up to one additional year), the Bank has engaged an independent consultant to (a) provide guidance to the Bank in connection with its achievement of tasks necessary to complete remediation contemplated by the 2012 Consent Order and 2014 Consent Order, and (b) assist the Department in reviewing the remediation of the Bank's compliance programs, including its sanctions compliance programs (the "Independent Consultant"). The Department has selected the Independent Consultant in the exercise of its sole discretion pursuant to the 2018 Consent Order.

57. Pursuant to the 2018 Consent Order, the Bank and the Independent Consultant have agreed to a workplan that will guide the objectives, responsibilities and activities of the Independent Consultant. However, the Department retains and shall exercise sole discretion to direct the course of the Bank's remediation efforts pursuant to the 2012 Consent Order, 2014 Consent Order, 2016 Supplemental Consent Order, 2018 Consent Order, and this Consent Order.

58. All other terms and conditions of the 2012 Consent Order, 2014 Consent Order, 2016 Supplemental Consent Order, and the 2018 Consent Order remain in full force and effect.

Sanctions Compliance Plan

59. Within ninety (90) days of the conclusion of the term of the Independent Consultant (including any extension pursuant to Paragraph 56 above), the Bank shall submit to the Department a written plan, acceptable to the Department, to improve and enhance the Bank's compliance with applicable OFAC and New York laws and regulations relating to sanctions compliance (the "Sanctions Compliance Plan"). At a minimum, the Sanctions Compliance Plan shall include the following:

a. an annual assessment of OFAC compliance risks arising from the global business activities and customer base of the Bank's subsidiaries, including risks arising from transaction processing and trade finance activities conducted by or through the Bank's global operations;

b. policies and procedures to ensure compliance with applicable OFAC Regulations by the Bank's global business lines, including screening with respect to transaction processing and trade financing activities for the direct and indirect customers of Bank subsidiaries;

c. the establishment of an OFAC compliance reporting system that is widely publicized within the global organization and integrated into the Bank's other reporting systems in which employees report known or suspected violations of OFAC regulations, and that includes a process designed to ensure that known or suspected OFAC violations are promptly escalated to appropriate compliance personnel for appropriate resolution and reporting;

d. procedures to ensure that the OFAC compliance elements are adequately staffed and funded;

e. training for the Bank's employees in OFAC-related issues appropriate to the employee's job responsibilities that is provided on an ongoing, periodic basis; and

f. an audit program designed to test for compliance with OFAC Regulations.

60. To the extent that the Bank has already created some part or all of the plan required in Paragraph 59 a. through f. above, any plan submitted pursuant to these Paragraphs 59-60 may identify such prior plan, and reference the relevant updates or revisions to such policies, procedures and processes called for by subparagraphs a. through f.

Corporate Oversight Plan

61. Within ninety (90) days of the conclusion of the term of the Independent Consultant (including any extension pursuant to Paragraph 56 above), the Bank shall submit to the Department a written plan, acceptable to the Department, to enhance oversight, by the management of the Bank and the New York Branch, of the Bank's and the New York Branch's compliance with applicable OFAC and New York laws and regulations relating to sanctions compliance (the "Sanctions Corporate Oversight Plan"). The Sanctions Corporate Oversight Plan shall provide for a sustainable governance framework that, at a minimum, addresses, considers and includes:

a. actions the board of directors will take to maintain effective control over compliance with both OFAC laws and regulations and related New York laws and regulations;

b. measures to improve the management information systems reporting of the Bank's compliance with both OFAC laws and regulations and related New York laws and regulations to the senior management of the Bank;

c. clearly defined roles, responsibilities, and accountability regarding compliance with both OFAC laws and regulations and related New York laws and regulations for the Bank's management, compliance personnel, and internal audit staff;

d. measures to ensure that the person or groups at the Bank charged with the responsibility of overseeing the Bank's compliance with both OFAC laws and regulations and related New York laws and regulations possess appropriate subject matter expertise and are actively involved in carrying out such responsibilities; and

e. adequate resources to ensure compliance with this Order.

62. To the extent that the Bank has already created some part or all of the plan required in Paragraph 61 a. through e. above, any plan submitted pursuant to these Paragraphs 61-62 may identify such prior plan, and reference the relevant updates or revisions to such policies, procedures and processes called for by subparagraphs a. through e.

Progress Reports

63. For a period of two years following the conclusion of the term of the Independent Consultant (including any extension pursuant to Paragraph 56 above), Standard Chartered shall, within thirty (30) days of the end of each six-month period, submit to the Department a written progress report detailing the form and manner of all actions taken to secure compliance with the provisions of this Order and the results thereof, including, but not limited to, Paragraphs 59-62 above.

Full and Complete Cooperation of Standard Chartered

64. Consistent with applicable law, the Bank agrees it will fully cooperate with the Independent Consultant and support its work by, among other things, providing the Independent Consultant with access to all relevant personnel, consultants and third-party service providers, files, reports, or records. The Bank further commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Breach of the Consent Order

65. In the event that the Department believes Standard Chartered to be in material breach of the Consent Order, or any provision hereof, the Department will provide written notice of the breach(es) to Standard Chartered and Standard Chartered shall, within ten (10) business days of receiving such notice, or on a later date if so determined in the Department's sole

discretion, appear before the Department to demonstrate that no material breach occurred or, to the extent pertinent, that the breach has been cured to the satisfaction of the Department.

66. The parties agree that Standard Chartered's failure to make the required showing within the designated time period shall be presumptive evidence of the Bank's breach. Upon a finding that Standard Chartered has breached the Consent Order, Standard Chartered agrees that the Department shall have all remedies available to it under the New York Banking and Financial Services laws and regulations and may make use of any evidence available to the Department in any ensuing hearings, notices, or orders. Standard Chartered submits to the jurisdiction of the Department for any such future proceedings.

Waiver of Rights

67. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal or agency outside the Department.

Parties Bound by the Consent Order

68. This Consent Order is binding on the Department and Standard Chartered, as well as any successors and assigns. This Consent Order does not bind any foreign, federal or other state agency or any law enforcement authority.

69. No further action will be taken by the Department against Standard Chartered for the specific conduct set forth in this Consent Order, provided that the Bank fully complies with the terms of this Consent Order.

70. Notwithstanding any other provision of the Consent Order, the Department may undertake action against Standard Chartered for transactions or conduct that Standard Chartered did not disclose to the Department in the written material Standard Chartered has submitted to the Department in connection with this matter.

Notices

71. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Megan Prendergast Millard
Deputy Superintendent for Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Elizabeth Nochlin
Director, Investigations and Intelligence and
Senior Assistant Deputy Superintendent for Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Samantha Jacobson
Excelsior Fellow
New York State Department of Financial Services
One State Street
New York, NY 10004

For Standard Chartered:

Scott Corrigan
General Counsel, Europe & Americas
Standard Chartered Bank
1095 Avenue of the Americas
New York, NY 10036

Miscellaneous

72. Each provision of this Consent Order shall remain effective and enforceable against Standard Chartered, its successors and assigns until stayed, modified, suspended, or terminated by the Department.

73. No promise, assurance, representation or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of the Consent Order.

[*remainder of page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed this 9th day of April, 2019.

STANDARD CHARTERED BANK

By: _____
BILL WINTERS
Group Chief Executive

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: _____
LINDA A. LACEWELL
Acting Superintendent of Financial Services

STANDARD CHARTERED BANK, NEW YORK BRANCH

By: _____
TORRY BERNTSEN
Chief Executive Officer, Americas

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: _____
MATTHEW L. LEVINE
Executive Deputy Superintendent for Enforcement